LAUR-02-5545

Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs

Roger G. Johnston and Anthony R.E. Garcia

Vulnerability Assessment Team
Los Alamos National Laboratory
MS J565, Los Alamos, New Mexico 87545, USA
505-667-7414 rogerj@lanl.gov

Abstract

The Vulnerability Assessment Team at Los Alamos National Laboratory has conducted a large number of vulnerability assessments on security devices, systems, and programs for various government agencies and private companies. This work has led us to develop generic recommendations and suggestions for conducting effective vulnerability assessments. We offer these not as rigorous, hard and fast rules, but rather as a starting point for discussion, analysis, and self-assessment. We also identify some of the common problems and barriers to effective vulnerability assessments and physical security. We conclude with a simplistic, but hopefully useful, self-assessment survey for evaluating the health of a given physical security program.

Introduction

The Vulnerability Assessment Team[1] (VAT) at Los Alamos National Laboratory (LANL) has conducted vulnerability assessments on over 200 security devices in the last few years, primarily in the area of tamper and intrusion detection.[2] The VAT has also analyzed security programs and procedures for over two-dozen government agencies and private companies, much of it in the area of nuclear security. As a result of this work, we have identified what we believe to be some of the attributes of an effective vulnerability assessment, and this has led to a set of general recommendations.

We do not view these recommendations as being rigidly cast in stone, nor do we consider them exhaustive. Not all of our recommendations will be automatically germane to any given physical security device, system, or program. In fact, many of them should NOT be applied to routine, low-level security applications. We also do not attempt here to significantly argue for, or even to substantially motivate, these recommendations. To do so would require lengthy and detailed discussions. Instead, we view our recommendations as a starting point for discussion, analysis, and self-evaluation of physical security effectiveness.

This paper is organized as follows: We first review some of the reasons why physical security is such a difficult challenge. A vulnerability assessment cannot be effective, in our view, without appreciating this fact. Next, we discuss why vulnerability assessments themselves are tricky, and list some of the barriers that get in the way. Our recommendations and suggestions for effective vulnerability assessments follow. We conclude the paper with an admittedly superficial, but we hope still thought provoking, "self evaluation survey" for security managers involved with high-security applications, such as the protection of nuclear materials.

Why is Physical Security so Difficult?

Physical security involves protecting valuable physical assets from harm. This harm can involve theft, destruction, sabotage, vandalism, espionage, forgery, counterfeiting, or tampering. The task of reliably protected against harm is a daunting one. Recognition of this fact is essential because complacency, overconfidence, or arrogance are incompatible with good security, or with good vulnerability assessments.

One of the reasons that physical security is so difficult is that it is highly multidimensional.[3,4] Whereas an adversary need only find and exploit one or a small number of vulnerabilities to succeed, physical security managers must identify, understand, and manage all possible vulnerabilities. While adversaries can attack at only one or a small number of points, security managers must often protect large, spatially distributed facilities. They must plan for all possible attacks at unpredictable times from all possible adversaries, many of whom may be completely unknown. Whereas security personnel are generally constrained by legal, ethical, humane, and public relations considerations, their adversaries (e.g., terrorists) may not be.

Another serious challenge for physical security is the general lack of useful performance measures. The traditional performance measure for security is pathological: success is defined as

nothing happening. This kind of performance measure does not permit effective cost/benefit analysis, and often results in insufficient resources being made available for security. Moreover, it tends to result in irrational cyclical fluctuations in security funding. Security budgets typically decay over time as long as there are no major security incidents. Once a major incident occurs, however, hysteria tends to ensue. Massive resources are suddenly thrown at the problem, much of them ultimately wasted. Draconian and often downright silly measures are introduced, some of which actually decrease overall security, or at least divert attention from more effective measures. (Thus, for example, we see airport security personnel after September 11th confiscating fingernail clippers—presumably to keep would-be terrorists from threatening airplane passengers and pilots with bad manicures.) Once a security crisis passes, the emphasis on physical security typically again erodes away until the next serious incident, at which point another frantic spike in funding and activity occurs.

Effective physical security is also hampered by a lack of standards. The few standards that do exist are of little value. Standards, however, are not automatically a guarantee of effective security. If they are too broad or too narrow, not well thought through, and/or mindlessly applied, they can cause more harm than good. Moreover, there is the potential problem referred to in the old engineering joke: that the great thing about standards is that there are so many to choose from!

Physical security is also commonly plagued by ambiguity. Security programs are frequently quite vague as to exact goals and adversaries.[5] Not helping the problem is the fact that security terminology is often sloppy, misleading, misunderstood, or misused, even by experienced security professionals.[5]

Attitude can be a particularly significant problem for a physical security program. While there are potential benefits to showing great confidence to the outside world (because this may discourage adversaries), a healthy security program does not believe its own public guarantees and assurances. Far too often, however, physical security managers, and the high-level personnel they report to, believe their own press releases. Ominously, many security programs retaliate against insiders or outsiders who question security measures, offer suggestions, or call for improvements. Physical security is a very difficult assignment under the best of circumstances. Security managers and security programs cannot afford to ignore, as they often do, suggestions and criticisms from any quarter—and especially from their own personnel. Even fanciful comments and suggestions from amateurs and outsiders can be useful in that they permit insight into the thought processes of potential adversaries.

Other problems that typically add to the difficulty of providing effective physical security include society's ambivalent attitudes towards security, the multidisciplinary and (increasingly) technological nature of physical security, the relatively low status and educational level of many security workers, the boredom often associated with routine security functions, and the tendency for the field to attract linear/concrete thinkers, authoritarians, and bureaucrats.[3] "Compliance mode" can also be a major problem. This involves security managers or other security personnel being so focused on satisfying superiors, auditors, regulators, bureaucrats, and formal security requirements that they lose sight of real-world security threats. Being distracted by paperwork and busywork is a serious problem with physical security which, first and foremost, needs to be about paying attention. Compliance mode is very difficult to avoid in large organizations and bureaucracies, in well-established operations, and for security programs that do not encourage security personnel to be flexible, creative, introspective, clever, and proactive (and that do not have senior officials with these attributes).

Why are Vulnerability Assessments so Difficult?

A vulnerability assessment is an attempt to discover and demonstrate weaknesses in a security device, system, or program.[6] Often, it also includes suggesting possible counter-measures. Vulnerability assessments are difficult for a lot of different reasons. One major hindrance is the prevalence of an absolutist, binary view of security.[5] Too many people (including security managers) believe a security device, system, or program is either secure, or else it has vulnerabilities and is thus insecure. In reality, however, security is a continuum. Nothing is either fully secure or completely insecure. Vulnerabilities always exist, and not all of them can ever be fully known or eliminated.

In many cases, security managers and supervisors, as well as manufacturers and vendors of security products, do not want vulnerability assessments done because they uncover problems. The discovery of vulnerabilities is viewed as bad news even though, ideally, it should be viewed as good news. After all, only when a vulnerability is found can it be mitigated or eliminated.

Similarly, security managers often view implementing security improvements or vulnerability counter-measures as a shameful admission of previous negligence or incompetence, rather than as an indication of a process of ongoing improvement. There is also frequently a "shoot the messenger" mentality.[7] Vulnerability assessors (called "blackhatters"!) are often viewed by security managers and organizations as a threat, rather than the adversaries and the vulnerabilities that the assessors uncover.

Vulnerability assessments themselves are quite complex. There are no generally useful guidelines or standards for how to do a vulnerability assessment.[8] Time and funding are often quite limited, although adversaries who attack a security device or program may not be so constrained. A time- or budget-limited vulnerability assessment, moreover, requires some kind of prioritization of the hundreds of possible attacks. Time and money will usually not be available to study them all. Not all possible attacks will be relevant or ultimately prove to be successful, and some of the attacks that do ultimately work may end up consuming more time and money to develop than they are worth. There are usually no obvious ways to prioritize attacks, though experience seems to be helpful.

A related complication is that we don't automatically know when the best attacks have been found during a vulnerability assessment. The best attacks may go forever undiscovered, or be discovered only at a later date by a different set of vulnerability assessors (or adversaries). Vulnerability assessments thus have no clear-cut end point. It is also often quite difficult to obtain high levels of realism when exploring, testing, or demonstrating security vulnerabilities. This is particularly true inside high security facilities. Another complicating factor is that defeating a security device, system, or program is a matter of degree and of probability, not absolute certainty. A crude attack will not necessarily fail with 100% probability, nor will a subtle attack always succeed. Estimating the degree and probability of a security defeat is not a simple matter.

Many real-world attacks on security devices/systems/programs rely on false alarming, fault analysis, "poke the system", "watch and pounce", or social engineering methods.[4] Because these

types of attacks tend to be anomalous, rare or random events, they can be quite difficult for vulnerability assessors to observe, model, predict, or replicate. It can also be difficult to sufficiently control related parameters, and to model or predict complicated human factors.

(False alarming is an attack where the adversary induces random, multiple false alarms in order to undermine the usefulness of the security and the confidence placed in it. Fault analysis involves an adversary deliberately causing the device or system to perform in a manner different from the way it was intended in order to learn useful information that can be exploited. Fault analysis attacks can be particular effective against complex, or high-tech devices or systems. "Poke the system" attacks involve the adversary probing the security, seeing what happens, and then using what was learned. With "wait and pounce", the adversary passively waits until security personnel make a mistake, then quickly jumps into action to exploit that mistake. "Social engineering" is the term used for attacks that relay on compromising key personnel through persuasion, seduction, bribery, impersonation, threats, or force.)

While vulnerabilities in physical security often involve various hardware factors, effective physical security is really more about human factors, behaviors, and psychology. Indeed, physical security usually fails not because of hardware problems, but fundamentally due to human errors and foibles, stupidity, laziness, wishful thinking, over confidence, arrogance, a lack of attention or imagination, poor training and communication, or an unwillingness to commit sufficient resources to protection. These are difficult variables to study and characterize.

Other common problems that can interfere with effective vulnerability assessments include[5] conflicts of interests on the part of the assessors, "recursion" (chasing a moving target when implementing recommended counter-measures would introduce new vulnerabilities), uncertainties about how to best report results, the complex interaction between different layers of security,[4] the difficulty of maintaining realism when testing security, and the need to maintain safety and security while doing so.

Recommendations for Effective Vulnerability Assessments

Here—in no particular order—are our general recommendations and suggestions (based on our experiences) for how to conduct an effective vulnerability assessment of a security device, system, or program:

1. Vulnerability assessments should include not just discovering and demonstrating vulnerabilities, but also suggesting possible counter-measures and effective procedures. Security managers are usually more willing to try to deal with a vulnerability if at least some tentative, potential solutions or partial solutions can be offered as early as possible.

2. A vulnerability assessment should be done iteratively, throughout the design process for a new security device or system (including at the earliest stages), not just at the end when it is difficult politically, psychologically, programmatically, and technically to make necessary changes.

3. Ideally, completely different vulnerability assessors should then analyze the security device/system and the proposed use protocols when the new device/system is completed, using information from the vulnerability assessments conducted throughout the design process.

4. Periodic vulnerability assessments should be done throughout the life of a security device, system, or program.

5. Vulnerability assessments should be undertaken by personnel who are independent, imaginative, and psychologically predisposed to finding problems. Assessors who do not consciously or unconsciously want to find vulnerabilities are unlikely to do so. Ideally, the vulnerability assessors should have a track record of discovering and demonstrating security vulnerabilities, and suggesting effective counter-measures. Assessors must be free of any conflicts of interest (e.g., they must not be the inventor, developer, promoter, vender, or manufacturer of the device or system), and must be under no pressure, undue influence, or unrealistic constraints (including time) regarding their analysis, findings, recommendations, or the types of attacks they can consider.

6. Undiscovered vulnerabilities always exist. A vulnerability assessment that finds no vulnerabilities is useless, must be rejected, and should be repeated using different assessors who will do the job correctly.

7. Security devices, systems, and programs do not "pass" a vulnerability assessment any more than people "pass" an IQ test. There are currently no meaningful standards for "certifying" a security device, system, or program in terms of vulnerabilities. Such standards may be very difficult to develop, as well as potentially dangerous if mindlessly or rigidly applied.

8. The discovery of new security vulnerabilities should be viewed as good news (since they can then be mitigated), not bad news.

9. Security personnel, supervisors, and managers, as well as developers, promoters, vendors, and manufacturers of security devices and systems, should not be penalized when new vulnerabilities are discovered.

10. Retaliation against vulnerability assessors, or any personnel (internal or external) who raise security concerns or questions is unacceptable, the sign of a pathological security program, and must not be tolerated.

11. Security devices are often only one part of an overall security system or program. Discovering vulnerabilities in a device does not necessarily mean that the entire system or program has failed. On the other hand, simply because a particular security device is but one, non-invincible part of an overall security system or program should not be used as an excuse to avoid optimizing its security (in a cost-effective manner).

12. Vulnerability assessors should report their findings and recommendations directly to relatively senior management in the sponsoring organization. The vulnerability assessment should not be interpreted, edited, or censored by low- or middle-level personnel (or intervening agencies) prior to reaching the most relevant managers.

13. If it is not possible to use external, professional vulnerability assessors because of financial limitations or security concerns, at least try to get clever, hands-on people in your organization to

think about how they would defeat your security. They do not necessarily have to be security professionals. Indeed, intelligent amateurs can sometimes spot problems that are overlooked by security professionals who are tightly focused on the routine and day-to-day details of security. One advantage of involving internal, non-security personnel in reviewing your security is that it can increase the awareness and appreciation of security throughout your organization.

14. To the extent practical, vulnerability assessments should be conducted in the context of the relevant and specific security applications, purposes, environment, economics, personnel, training, adversaries, and defeat consequences. Assessing the vulnerabilities in isolation of these factors limits the usefulness of the findings.

15. Protocols for hardware manufacture, procurement, storage, transport, installation, inspection, removal, disposal, and record keeping should all be carefully analyzed. The security of the hardware manufacturer, vendor, shipper, and receiving department must be carefully analyzed.

16. Vulnerability assessments should emphasize the simplest attacks and the weakest links in the chain of security. Complex, high-technology attacks are appropriate only after the low technology attacks have been thoroughly explored.

17. Effective vulnerability assessments are holistic. Conducting vulnerability assessments on pieces of a security device, system, or program is usually a waste of time, and will tend to lead to dangerous over-confidence and overlooked vulnerabilities.

18. Thorough vulnerability assessments of security devices require multiple copies of the device that can be destroyed during the analysis. Usually the more samples that are available, the more comprehensive the findings and the larger the number of discovered vulnerabilities.

19. Physical, environmental, ergonomic, field readiness, or materials testing of a security device—although very useful—is not the same thing as vulnerability assessment. These other kinds of tests should not be confused with vulnerability assessments, though they often are.

20. Vulnerability assessment must avoid the common tendency to underestimate the cleverness, knowledge, skills, dedication, and resources available to an adversary. (This is surely one of the lessons of September 11.)

21. Vulnerability assessments must not be given unrealistic constraints on possible attack tools, procedures, personnel, or strategies.

22. There must be a realization that adding one more layer of mediocre security to a system or program may actually decrease overall security.

23. All of the following types of attacks must be considered: false alarming, fault analysis, “poke the system”, “watch and pounce”, and social engineering methods. The latter includes attacks that involve the adversary impersonating government authorities, auditors, managers, security personnel, maintenance and craft workers, emergency response crews, law enforcement officers, etc.

24. All of the following adversaries must be considered: insiders, outsiders, and outsiders assisted by insiders.

25. It is essential to factor in Rohrbach's Maxim: No security system will ever be used properly (the way it was designed) all the time.[9]

26. It is essential to factor in Shannon's Maxim: The adversaries know and understand the security systems and hardware being used.[9]

27. Reporting Findings

A comprehensive vulnerability assessment report should consist of the following 5 items:

(A). A detailed description of the successful attacks. For each attack the following information should be provided:

- Is the attack theoretical, partially demonstrated, fully demonstrated but not perfected, or practiced to perfection?
- What are the cost, time, and effort to devise and demonstrate the attack?
- What time is required on-site to do the attack?
- How much time is required for the attack to become activated, which may differ from the time to do the attack?
- What time is required for off-site preparation?
- What personnel, skills, technical sophistication, and costs are necessary to complete the attack?
- How many times and for how long must the adversary have on-site access to the hardware or infrastructure being attacked?
- What is the size, weight, cost, and nature of the tools and materials that must be brought on-site for the attack?
- Is inside information necessary for the attack, or just what is publicly available?

(B). Sample(s) of the defeated security devices should be provided if practical and appropriate.

(C). The report should include a discussion of possible counter-measures and protocols for dealing with the vulnerabilities.

(D). Samples of the security devices employing any suggested design changes should be provided, if practical.

(E). The report should include a statistical summary of the assessment that is purged of sensitive or classified vulnerability and attack details, but that contains information on the identity of the persons/organization doing the vulnerability assessment, the level of effort for the vulnerability assessment, the number of successful attacks, time to develop them, time to execute them, type of defeats, number of possible counter-measures and their general nature. A developer, manufacturer, or user of a security device or system who claims that a particular device or system has undergone vulnerability assessment should make this summary available to anyone to whom that claim is being made.

The Attributes of an Effective Physical Security Program - Self Assessment

The self-assessment tool that appears below is a simplistic, but still hopefully useful, tool for quickly evaluating a given physical protection program, and for thinking more broadly about security issues. It is only relevant for high security applications.

Scoring is based on how many of the 38 statements below are valid for your security program. For each statement below that matches your security program, you score one point. You get zero points for a statement that does not apply to your program. The total number of points you score (0-38) is a rough measure of the health of your security program.

We—somewhat arbitrarily—rank scores as follows:

35-38 points: You have a top-notch security program!
28-34 points: There is room for significant improvement.
21-27 points: This is not a healthy security program.
10-20 points: Hopefully your security program involves guarding only candy bars!
Less than 10 points: Have you considered another line of work?

<u>How many of these statements are more or less true of your security program?</u>

1. There is no overconfidence. Effective security is viewed throughout the security program as a very difficult challenge, not as a sure thing.

2. Security is viewed as a continuum, not a binary state (i.e., either "secure" or "not secure").

3. It is widely recognized throughout the security program that satisfying auditors, superiors, and regulations is not automatically a guarantee of effective security, and can sometimes actually impede security.

4. Comments, suggestions, and criticisms concerning security are welcome and seriously considered from any quarter (internal or external) without invoking retaliation, undue defensiveness, or automatic cursory rejection of the input.

5. Undiscovered security vulnerabilities are always assumed to exist. The discovery of new security vulnerabilities is thus viewed as good news (since they can then be mitigated), instead of bad news.

6. Internal vulnerability assessments or security surveys are performed at least twice a year at all levels of the security program, and involve meaningful self-criticism.

7. Comprehensive, holistic vulnerability assessments are performed at least once a year by external, independent, and creative personnel. These vulnerability assessors have no conflicts of interest, and are under no pressure, undue influence, or unrealistic constraints regarding their analysis, findings, or recommendations.

8. Vulnerability assessments or security surveys (internal or external) **always** uncover vulnerabilities or areas for improvement.

9. Vulnerability assessors report their findings and recommendations directly to senior management.

10. Security personnel, supervisors, and managers are not penalized when new vulnerabilities are discovered.

11. Security personnel, including low-level personnel, are encouraged to point out vulnerabilities, raise questions and concerns, and offer creative suggestions—and frequently do so.

12. Security personnel feel comfortable reporting a security incident, anomaly, or problem, and are praised or rewarded for doing so. (No "shoot the messenger" syndrome.)

13. Security personnel, including low-level personnel, are encouraged to think about adversaries (internal or external) and how they might defeat the security program, and to share these ideas with coworkers, supervisors, and managers—and frequently do so.

14. Security personnel receive training and practice with observational skills. They receive periodic training on how to spot social engineering tactics, misdirection, and sleight of hand techniques.

15. Security personnel accept no food or drink from colleagues, co-workers, or unauthorized sources. Approved sources are secure.

16. The morale and self-esteem of security personnel is high.

17. Security personnel, including low-level personnel, are treated as professionals (with courtesy and respect), and are granted opportunities for training and professional advancement.

18. A grievance or complaint resolution process is in place for disgruntled workers (whether they be security personnel or otherwise). This process is effective, sincere, and fair—and is widely viewed as such by the work force.

19. Confidential, professional counseling is available for troubled workers (whether they be security personnel or otherwise).

20. Security personnel, including low-level personnel, are passionate about their role, responsibilities, and contributions.

21. Security personnel treat all facility personnel and visitors with courtesy, efficiency, and the highest levels of professionalism.

22. Security supervisors and managers are generally well respected by subordinates at all levels.

23. Security managers and supervisors frequently "walk the spaces", chat informally with low-level security personnel, and occasionally work low-level shifts alongside security personnel to gain a realistic understanding of security issues.

24. Security training exercises are realistic, useful, and fun.

25. Security personnel are frequently engaged in official contests, test of skill, and demonstrations of prowess.

26. "What if" mental exercises occur on a daily or weekly basis at all levels of the security program.

27. The consequences of a security failure are well understood by all security personnel, and these are discussed on a frequent basis.

28. Security personnel are briefed at the start of a shift, and checked for fitness of duty (even if this involves simply chatting with them to establish sobriety, coherence, fatigue level, and mental/emotional state).

29. Security personnel are thoroughly debriefed at the end of a shift, allowing an opportunity for incidents, problems, questions, and suggestions to be discussed.

30. Rosters, duty assignments, and schedules of work authorized inside the facility are well protected from tampering. Paper documents and verbal orders are not taken at face value.

31. Periodic, thorough background and reliability checks are performed on all security personnel, and on all personnel with access to critical protected assets.

32. Unexplained or unexpected absences of security personnel are investigated immediately, as are any sudden outbreaks of widespread illnesses.

33. Authorities, agency heads, high-level personnel, government officials, and VIPs are subject to the same security rules and processing as all other personnel and visitors.

34. Security personnel frequently discuss and rehearse all of the following attacks: internal, external, internal + external, false alarming, fault analysis, "poke the system", "wait and pounce", and social engineering.

35. Security personnel know exactly how and when to summon help or sound an alarm, and can do so reliably and quickly.

36. There are clear policies on the use of physical force (including lethal force and force against coworkers), these policies are frequently discussed in a "what if" format, and all security personnel understand these policies, rehearse them, and know what is expected of them.

37. Security managers and supervisors frequently test security, but without compromising it.

38. The health and safety of security personnel is a high priority. Significant insurance and medical coverage is in place for security personnel hurt or killed in the line of duty.

[1] LANL Vulnerability Assessment Team Home Page, <http://pearl1.lanl.gov/seals>.

[2] R.G. Johnston, A.R.E. Garcia, and A.N. Pacheco, "Efficacy of Tamper-Indicating Devices", Journal of Homeland Security, April 16, 2002, <http://www.homelandsecurity.org/journal/Articles/displaySciTech.asp?article=50>.

[3] D.L. June (Editor), "Protection, Security, and Safeguards: Practical Approaches and Perspectives", CRC Press, 2000, pp. 21-25, 80, 184-191.

[4] R. Anderson, "Security Engineering", Wiley (2001).

[5] R.G. Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", The Nonproliferation Review, Vol. 8, No. 1 (Spring 2001), pp. 102-115, <http://lib-www.lanl.gov/la-pubs/00367047.pdf>.

[6] R.G. Johnston and A.R.E. Garcia, "Analyzing Vulnerability Results for Tags and Tamper-Indicating Seals", Proceedings of the 2001 U.S. Army Conference on Applied Statistics, (in press).

[7] E. Hutchings, R. Leighton, R.P. Feynman, and A. Hibbs, 'Surely You are Joking, Mr. Feynman: Adventures of a Curious Character", Batam (1985), pp. 119-137.

[8] See, for example, R.G. Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals", Journal of Testing and Evaluation, Vol. 25 (July 1997), pp. 451-455, <http://lib-www.lanl.gov/la-pubs/00418792.pdf>.

[9] R.G. Johnston, "Cryptography as a Model for Physical Security", Journal of Security Administration, Vol. 24 (2001), pp. 33-43.